

משרד החינוך
המנהל הפדגוגי
אגף בכיר בחינוך
מחברת בחינה

לנבחנים ולנבחנות שלום,
יש לקרוא את ההוראות בעמוד זה ולמלא אותן בדיוקנות. אי-מילוי ההוראות עלול לגרום לתקלות ואף להביא לידי פסילת הבחינה.
הבחינה נועדה לבדוק הישגים אישיים, ולכן יש לעבוד עבודה עצמית בלבד. בזמן הבחינה אין להיעזר בזולת ואין לתת או לקבל חומר בכתב או בעל פה.
אין להכניס לחדר הבחינה חומר עזר – ספרים, מחברות, רשימות – חוץ מ"חומר עזר מותר בשימוש" המפורט בגוף השאלון או בהוראות מוקדמות של המשרד. כמו כן אין להכניס לחדר הבחינה טלפונים או מכשירים אלקטרוניים אחרים. שימוש בחומר עזר שאינו מותר יוביל לפסילת הבחינה.
לאחר סיום כתיבת הבחינה יש למסור את המחברת למשגיח ולעזוב בשקט את חדר הבחינה.

יש להקפיד על טוהר הבחינות!

הוראות לבחינה

- יש לוודא כי במדבקות הנבחן שקיבלת מודפסים הפרטים האישיים שלך. אין להוסיף או לשנות שום פרט במדבקות, כדי למנוע עיכוב בזיהוי המחברת וברישום הציונים.
- אם לא קיבלת מדבקה, יש למלא בכתב יד את הפרטים במקום המיועד למדבקת הנבחן.
- אסור לכתוב בשולי המחברת (החלק המקווקו) משום שחלק זה לא ייסרק.
- לטייטה ישמשו אך ורק דפי מחברת הבחינה שיועדו לכך.
- אין לתלוש או להוסיף דפים. מחברת שתוגש לא שלמה תעורר חשד לאי-קיום טוהר הבחינות.
- אין לכתוב שם בתוך המחברת משום שהבחינה נבדקת בעילום שם.

בהצלחה!

מדבקות נבחן והתאמות ملصقة ممتحن وملاءمات	מדבקות שאלון ملصقة نموذج امتحان
<div>שנה السنة חודש الشهر מועד موعد</div> <div>סמל ביה"ס מס' תעודת הזהות رقم المدرسة رقم الهوية</div>	
יש להדביק כאן ↑ מדבקות נבחן (ללא שם) يجب هنا ↑ إلصاق ملصقة ممتحن (بدون اسم)	
מדבקות לנבחן ملصقة ممتحن	

יש לסמן במשבצת ☐ אם ניתנה מחברת נוספת
يجب الإشارة في المربع إذا أُعطي دفتر إضافي
* التعليمات باللغة العربية على ظهر الصفحة

وزارة التربية والتعليم

القسم الكبير للامتحانات

الإدارة التربويّة

دفتر امتحان

تحيّة للممتحنين وللممتحنات،

يجب قراءة التعليمات في هذه الصفحة والعمل وفقاً لها بدقة. عدم تنفيذ التعليمات قد يؤدي إلى عواقب مختلفة وحتى إلى إلغاء الامتحان. أُعدّ الامتحان لفحص التحصيلات الشخصية، لذلك يجب العمل بشكل ذاتي فقط. أثناء الامتحان، لا يُسمح طلب المساعدة من الغير، ولا يُسمح إعطاء أو الحصول على موادّ مكتوبة أو شفهيّة. لا يُسمح إدخال موادّ مساعدة - كتب، دفاتر، قوائم - إلى غرفة الامتحان، ما عدا "موادّ مساعدة يُسمح استعمالها" المفضّلة في نموذج الامتحان أو في تعليمات مسبقة من وزارة التربية والتعليم. كما لا يُسمح إدخال هواتف خلويّة أو أجهزة إلكترونيّة أخرى إلى غرفة الامتحان. استعمال موادّ مساعدة لا يُسمح استعمالها سوف يؤدي إلى إلغاء الامتحان. بعد الانتهاء من كتابة الامتحان، يجب تسليم الدفتر للمراقب ومغادرة غرفة الامتحان بهدوء.

يجب التقيّد بنزاهة الامتحانات !

تعليمات للامتحان

1. يجب التأكّد بأنّ تفاصيلك الشخصية مطبوعة على ملصقات الممتحن التي حصلت عليها. لا يُسمح إضافة أو تغيير أيّة تفاصيل في الملصقات، وذلك لمنع عواقب في تشخيص الدفتر وفي تسجيل العلامات.
2. في حال عدم حصولك على ملصقة، يجب ملء التفاصيل في المكان المعدّ لملصقة الممتحن، بخطّ يد.
3. لا يُسمح الكتابة في هوامش الدفتر (في المنطقة المخطّطة)، لأنّه لن يتمّ مسح ضوئيّ لهذه المنطقة.
4. للمسوّدة تُستعمل أوراق دفتر الامتحان المعدة لذلك فقط.
5. يُمنع نزع أو إضافة أوراق. الدفتر الذي يُسلم ناقصاً يُثير الشكّ بعدم الالتزام بنزاهة الامتحانات.
6. لا يُسمح كتابة الاسم داخل الدفتر، لأنّ الامتحان يُفحص بدون ذكر اسم.

نتمنّى لكم النّجاح!

מדינת ישראל
משרד החינוך

סוג הבחינה: גמר לבתי-ספר לטכנאים ולהנדסאים
מועד הבחינה: אביב תשפ"ה, 2025
סמל השאלון: 735913
נספח: מילון מונחים

יישומי ניתוב IP ואבטחה ברשתות קמפוס

הוראות לנבחנים

א. משך הבחינה: ארבע שעות.

ב. מבנה השאלון ומפתח ההערכה: בשאלון זה שני פרקים:

פרק ראשון: יישומי ניתוב IP	45 נקודות
פרק שני: אבטחה ברשתות קמפוס	55 נקודות
סך-הכול	100 נקודות

ג. חומר עזר מותר בשימוש: מחשבון פשוט שאינו ניתן לתכנות, ואינו מאפשר להמיר ערכים בבסיסי ספירה שונים.

כל חומר עזר כתוב בכתב-יד או מודפס על נייר.

ד. הוראות מיוחדות:

- כתבו בעט בלבד.
- שאלון זה משמש כמחברת בחינה. כתבו את כל תשובותיכם בגוף השאלון, במקומות המיועדים לכך.
- עמודים 28-31 משמשים טיוטה לעריכת חישובים. כתיבת טיוטה בגוף השאלון או על דפים שמחוץ לשאלון עלולה לגרום לפסילת הבחינה.
- ענו על מספר השאלות הנדרש בכל פרק בהתאם להנחיות. המעריך יקרא ויעריך את מספר התשובות הנדרש בלבד לפי סדר כתיבתן, ולא יתייחס לתשובות נוספות.
- הדביקו את מדבקות הנבחן במקומות המיועדים לכך.
- בנספח לשאלון זה מובא מילון מונחים בשפות עברית, ערבית, אנגלית ורוסית. תוכלו להיעזר בו בעת הצורך.

שאלון זה משמש כמחברת בחינה. הדביקו את מדבקת הנבחן במקום המיועד לכך בעמוד 1 (כריכה קדמית).

בשאלון זה 32 עמודים ועמוד אחד של נספח

השאלות בשאלון זה מנוסחות בלשון רבים,
אף על פי כן על כל תלמידה וכל תלמיד להשיב עליהן באופן אישי.

בהצלחה!

המשך מעבר לדף

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

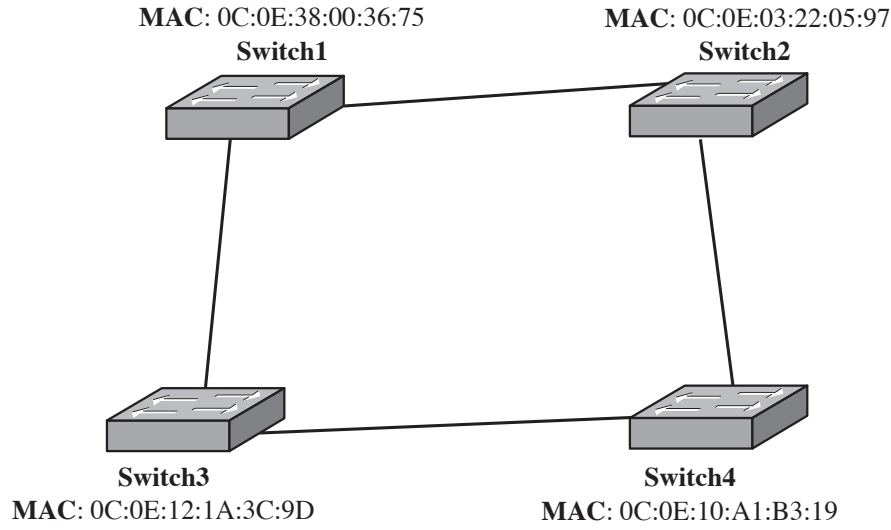
השאלות

כתבו את התשובות במקום המיועד לכך.
בשאלות רב-ברירה, לכל שאלה ארבע תשובות אך רק אחת מהן נכונה.
הקיפו בעיגול את הספרה המציינת את התשובה הנכונה.
בשאלות האחרות, פעלו על פי ההנחיות.

פרק ראשון: יישומי ניתוב IP (45 נקודות)
ענו על חמש עשרה מבין השאלות 1–18 (לכל שאלה – 3 נקודות).

שאלה 1

לפניכם טופולוגיה מספר 1, הכוללת ארבעה מתגים.
כל המתגים בעדיפות ברירת מחדל (default priority). לא הוגדרה עדיפות ב־bridge priority.



טופולוגיה מספר 1

איזה מתג ייבחר כ־root bridge?

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 2

מה תפקידו העיקרי של האלגוריתם DUAL ב-EIGRP?

- אחראי על חישוב המדד (Metric) של המסלולים.
- מבטיח שהרשת תהיה ללא לולאות ניתוב.
- אחראי על עדכון הנתבים השכנים.
- משמש לניהול אבטחת הרשת.

שאלה 3

מהי ההגדרה של "הניתוב הסטטי הצף" (floating static route) החוקי שיופעל כאשר נתיב EIGRP שהוגדר אינו זמין?

- `ip route 192.168.1.0 255.255.255.0 gig0/0 100`
- `ip route 192.168.1.0 0.0.0.255 192.168.2.2 90`
- `ip route 192.168.1.0 255.255.255.240 gig0/0 1`
- `ip route 192.168.1.0 255.255.255.224 10.0.0.0 90`

שאלה 4

איזו פקודה, מהפקודות שלפניכם, נדרשת כדי לפרסם את תת הרשת 192.168.1.0/28 לנתבים השכנים באזור 0 בפרוטוקול OSPF?

- `network 192.168.1.0 0.0.0.0 area 0`
- `network 192.168.1.0 255.255.255.224 area 0`
- `network 192.168.1.0 255.255.255.240 area 0`
- `network 192.168.1.0 0.0.0.15 area 0`

שאלה 5

לפניכם היגדים המתייחסים ל-LSDB (Link State Database).

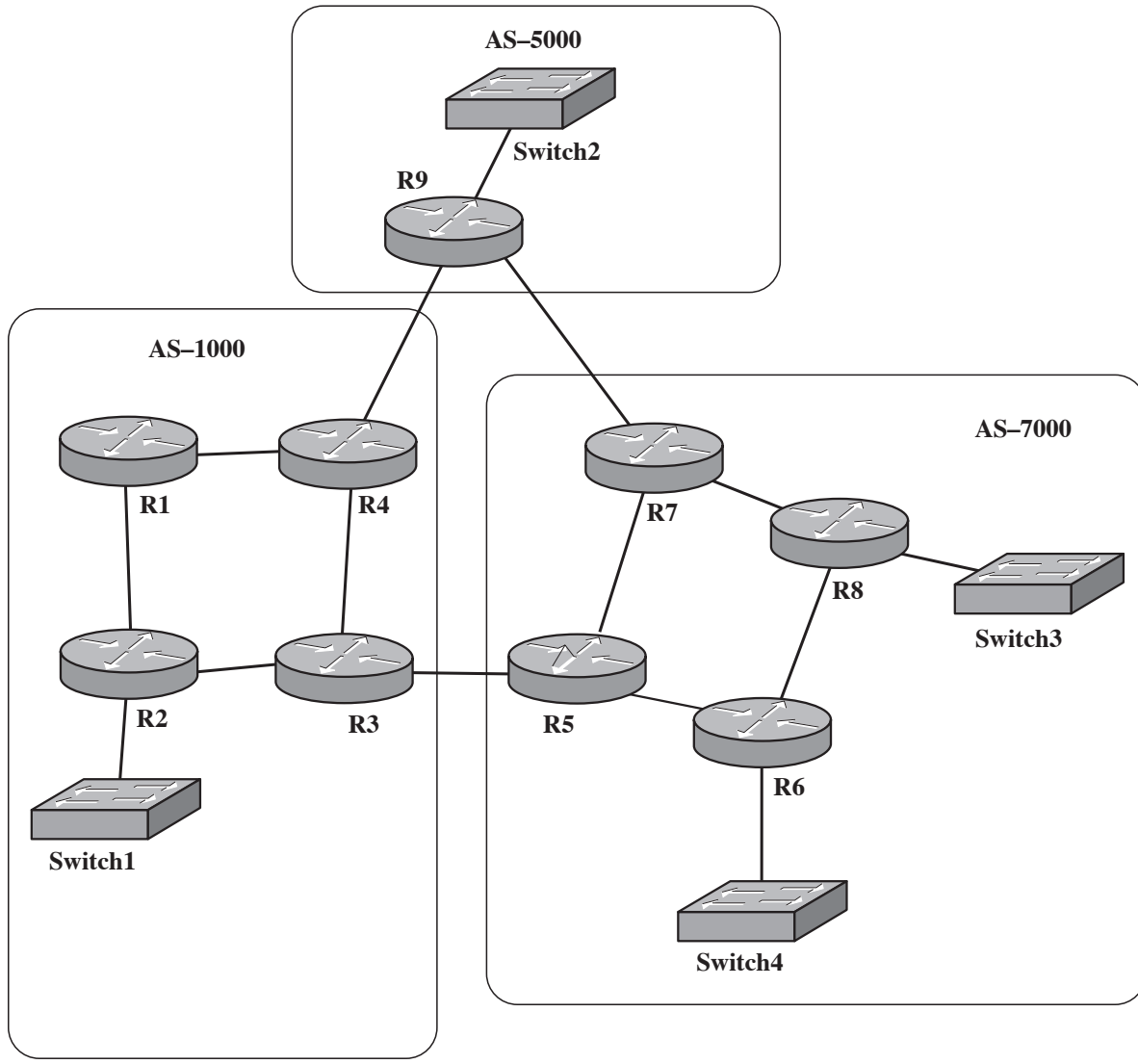
קבעו לגבי כל אחד מהם אם הוא נכון או לא נכון:

- | | |
|---|----------------|
| (א) כל נתב בתוך אותו אזור OSPF שומר עותק זהה של LSDB. | נכון / לא נכון |
| (ב) LSDB אינו תלוי בגודל הרשת ולא במספר הנתבים. | נכון / לא נכון |
| (ג) LSDB משמש רק לאיתור הנתבים הקצרים ביותר. | נכון / לא נכון |
| (ד) Virtual Links מגדיל את גודל ה-LSDB. | נכון / לא נכון |

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 6

לפניכם טופולוגיה מספר 2 עם שמות הנתבים. בכל הנתבים הוגדר הפרוטוקול BGP.



טופולוגיה מספר 2

כתבו את שמות הנתבים המשמשים כ-EBGP (Exterior BGP):

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 7

איזו תכונה (attribute) **איננה** משמשת לבחירת הניתוב בפרוטוקול BGP?

א. AS-path (Autonomous System)

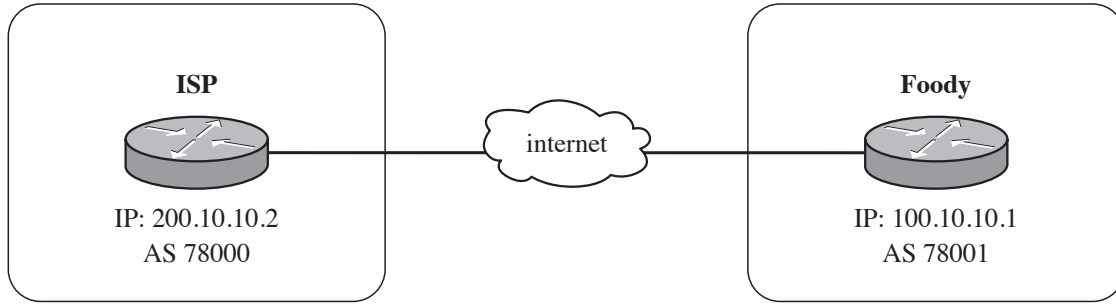
ב. TTL (Time to Live)

ג. Local Preference

ד. MED (Multi-Exit Discriminator)

שאלה 8

לפניכם **טופולוגיה מספר 3**, המתארת חיבור בין רשת חברת מזון Foody לספק האינטרנט ISP. פרוטוקול הניתוב שהוגדר ביניהם הוא BGP.



טופולוגיה מספר 3

השלימו את הפקודות הנדרשות בכל אחד מנתבי הקצה כדי שהפרוטוקול BGP יפעל כנדרש.

ISP Router: neighbor _____ remote-as _____

Foody Router: neighbor _____ remote-as _____

שאלה 9

איזה מהמאפיינים שלפניכם **איננו** מאפיין של פרוטוקולי ניתוב מסוג Link-state?

א. שמירת מפה מלאה של כל הטופולוגיה בכל נתב.

ב. שימוש באלגוריתם דיאקסטרה (Dijkstra) לחישוב המסלולים ליעד.

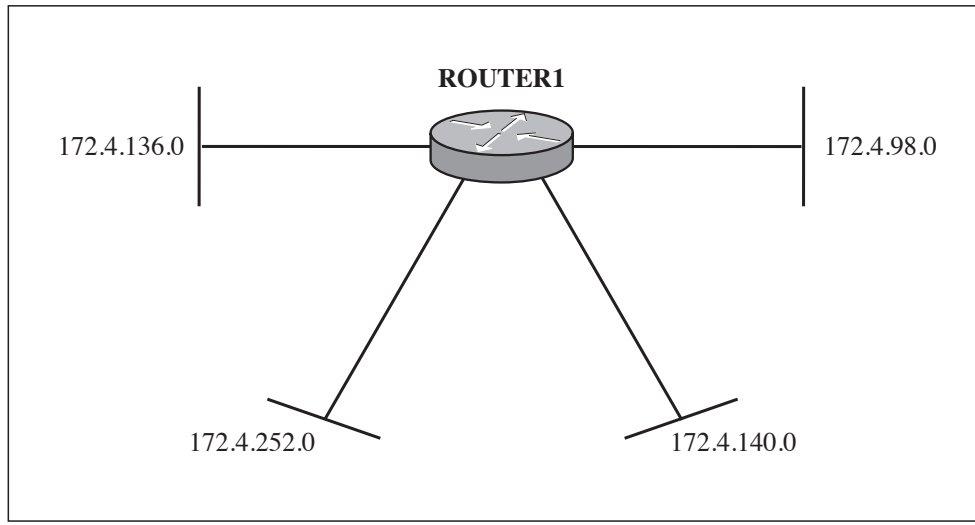
ג. שיתוף מידע של כל נתב רק עם הנתבים השכנים לו.

ד. התכנסות (converges) מהירה יותר מאשר פרוטוקולים הפועלים בשיטת Distance Vector.

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 10

לפניכם **טופולוגיה מספר 4**. לנתב Router1 מחוברות ארבע תתי רשתות, שכתובותיהן מופיעות בטופולוגיה. מסכת הרשת של כל תתי הרשתות היא: 255.255.254.0 .



טופולוגיה מספר 4

ענו על סעיפים א' ו-ב'.

- א) כמה מארחים (Hosts) מותרים לשימוש ניתן להגדיר בכל תת־רשת? _____
- ב) מהן כתובת ה-IP והתחילית (prefix) שיפורסמו על־ידי הנתב Router1 לאחר סכימת הרשתות (Route summarization)? _____

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלות 11-12 מתייחסות לפלט מספר 1 שלפניכם, המציג את תוצאת הפקודה show ip protocols שנכתבה בנתב מסוים:

```

Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
    Automatic network summarization is in effect
    Automatic address summarization:
    Maximum path: 4
    Routing for Networks:
      192.168.7.0
      192.168.1.0
      192.168.8.0
    Routing Information Sources:
      Gateway         Distance      Last Update
      192.168.7.1      90            813546
      192.168.1.1      90            819078
      192.168.8.1      90            851543
    Distance: Internal 90 external 170
  
```

פלט מספר 1

שאלה 11

מה משמעות המספר 100, המופיע בשורה הראשונה בפלט מספר 1?

- מספר ה-Router-ID.
- מזהה הרשת האוטונומית (Autonomous System).
- האזור (Area) שבו מופעל ה-EIGRP.
- המרחק הניהולי (administrative distance) של ה-EIGRP.

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 12

(א) מה יקרה אם נשנה את ערכו של K1, המופיע בשורה 6, ל- $K1 = 10$?

1. יוגדר טווח מקסימלי של 10 ק"מ עד לנתב הבא.
2. יגדל משקל ההשהיה (Delay) על המדד (Metric).
3. יגדל משקלו של רוחב הפס (bandwidth weight) בחישוב ה-Metric.
4. יקטן משקלו של רוחב הפס (bandwidth weight) בחישוב ה-Metric.

(ב) השלימו את הפקודה שתשנה את ערכו של K1 ל-10 (שאר הערכים יישארו כפי שמופיעים בפלט).

Router(config)#router _____

Router(config-router)#metric _____

שאלה 13

לפניכם פלט מספר 2, המציג פלט חלקי של הפקודה show ip eigrp neighbors שנכתבה בנתב:

H	Address	Interface	Hold Uptime {sec}	SRTT (ms)	RTO	Q Cnt	Seq Num
0	192.168.4.2	Fa4/0	10 00:10:02	40	1000	0	14
1	192.168.5.2	Fa5/0	11 00:08:26	40	1000	0	22
2	192.168.1.2	Fa0/0	11 00:01:37	40	1000	0	20

פלט מספר 2

(א) מה משמעות הערך SRTT (הנמדד במילי-שניות) שבטבלת פלט מספר 2?

1. הזמן שנמדד מרגע היציאה של הודעת EIGRP מנתב המוצא לנתב השכן, עד לקבלת אישור (Ack) בנתב המוצא.
2. הזמן שנמדד מרגע היציאה של ICMP PING מנתב המוצא למחשב היעד, עד לקבלת ICMP reply ממחשב היעד לנתב המוצא.
3. הזמן שנמדד מרגע היציאה של חבילה מנתב המוצא עד להגעתה למחשב היעד.
4. הזמן שממתין הנתב לפני שליחת הודעת Hello לנתב השכן.

(ב) על-פי פלט מספר 2, מהו משך הזמן (בשניות) שחלף מאז שנוצר קשר השכנות (Neighbor Adjacency) בין הנתב הנוכחי לנתב המחובר אליו בממשק Fa5/0 (interface)?

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 14

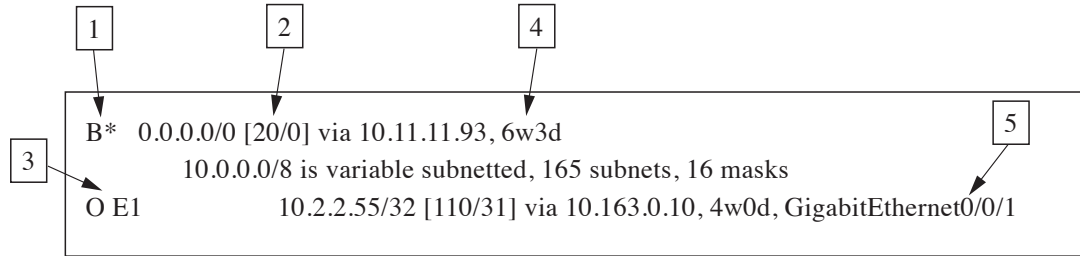
לפניכם היגדים המתייחסים לפרוטוקול HSRP (Hot Standby Router Protocol).

קבעו לגבי כל אחד מהם אם הוא נכון או לא נכון:

- נכון / לא נכון
- א) HSRP מאפשר חיבור בין שני נתבים בלבד.
- ב) הנתב הראשי (Active Router) ב-HSRP נבחר על-פי הערך הגבוה ביותר של ה-priority.
- ג) בכל קבוצה של HSRP חייב להיות לפחות נתב אחד שמוגדרת בו כתובת IP ציבורית.
- ד) HSRP פועל רק בשכבה השנייה (Data-Link Layer) במודל ה-OSI.
- ה) בתהליך הבחירה של הנתב הראשי (Active Router) ב-HSRP, חבילות Hello messages משמשות לשמירה על שכנות בין הנתבים בקבוצת HSRP ולגילוי תקלות.
- נכון / לא נכון

שאלה 15

בפלט מספר 3 נתון פלט חלקי של טבלת ניתוב מסוים. חלק מהמושגים המופיעים בפלט סומנו במספרים 1-5.



פלט מספר 3

כתבו מימין לכל אחד מהמושגים הבאים, את המספר המתאים לו מבין המספרים המופיעים בפלט מספר 3:

timestamp (route lifetime) - חותמת זמן שהנתיב ידוע.

administrative distance - מרחק ניהולי.

outbound interface - ממשק מעבר הנתונים.

route source (default route) - נתיב ברירת המחדל.

External route connection - נתיב המוביל לרשת שאינה באותו AS של הנתב הנוכחי.

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 16

לפניכם פלט מספר 4 שמציג את תוכן הפקודה show ip interface brief בנתב שהוגדר בו OSPF:

Router#show ip interface brief					
Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.1.1	YES	NVRAM	up	up
FastEthernet1/0	unassigned	YES	NVRAM	administratively down	down
Serial2/0	unassigned	YES	NVRAM	administratively down	down
Serial3/0	unassigned	YES	NVRAM	administratively down	down
FastEthernet4/0	192.168.4.1	YES	NVRAM	up	up
FastEthernet5/0	192.168.5.1	YES	NVRAM	down	down
GigabitEthernet6/0	172.16.1.1	YES	NVRAM	up	up
Loopback0	207.207.2.3	YES	NVRAM	up	up
Router#					

פלט מספר 4

על-פי הפלט, מה יהיה ה-Router ID?

שאלה 17

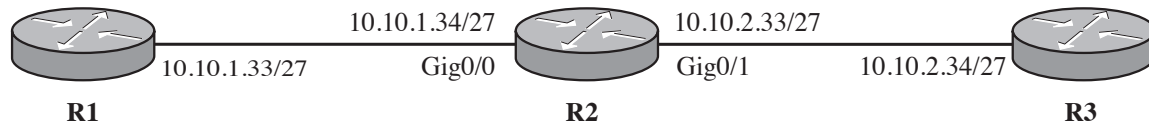
באיזה אלגוריתם משתמשים בדרך כלל לחישוב המסלולים בפרוטוקולי Distance Vector?

- א. Dijkstra
- ב. Bellman-Ford
- ג. SPF
- ד. Diffie-Helman

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 18

לפניכם טופולוגיה מספר 5, ובה שלושה נתבים שהוגדר בהם הפרוטוקול OSPF, וכן הפלט החלקי של נתב R2 בטופולוגיה (פלט מספר 5).



טופולוגיה מספר 5

```
hostname R2
!
interface Gig0/0
    ip address 10.10.1.34 255.255.255.224
!
interface Gig0/1
    ip address 10.10.2.33 255.255.255.224
!
router ospf 1
network 10.10.1.0 0.0.0.255 area 0
network 10.10.2.0 0.0.0.255 area 0
!
passive-interface Gig0/0
```

פלט מספר 5

על-פי טופולוגיה מספר 5 ופלט מספר 5 – מה נכון לומר לגבי נתב R2?

- נתב R2 לא ייצור יחסי שכנות עם נתב R3.
- נתב R2 לא ייצור יחסי שכנות עם נתב R1.
- נתב R2 ישלח ויקבל חבילות hello לנתב R3.
- נתב R2 ישלח עדכוני ניתוב OSPF לנתב R3.

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

פרק שני: אבטחה ברשתות קמפוס (55 נקודות)

ענו על עשרים ושתיים מבין השאלות 19–42 (לכל שאלה – 2.5 נקודות).

שאלה 19

איזו התקפה מבין הבאות לא שייכת ל-Reconnaissance attack?

- א. Social Engineering
- ב. Phishing
- ג. Port scan attack
- ד. Denial of Service

שאלה 20

בפרוטוקול STP, מהו "Path Cost"?

- א. מדד למרחק הלוגי בין מתגים (Switches).
- ב. מדד למרחק הלוגי בין נתבים (Routers).
- ג. משקל שניתן למתג בתהליך בחירת ה-Root Bridge.
- ד. זמן התגובה של המתג.

שאלה 21

איזה סיכון יכול להתרחש כאשר הרבה ממשקים במתג (Switch) מוגדרים כ-Trunk, ולא קיימות הגדרות אבטחה מתאימות?

- א. התקפות מסוג Phishing (דיוג)
- ב. התקפות מסוג Denial of Service (DoS) על הפרוטוקול VTP
- ג. VLAN Hopping – גישה לא מורשית ל-VLANs אחרים
- ד. חשיפת המתג למתקפות המתייחסות ל-DHCP (כגון תשובות DHCP לא מאושרות).

שאלה 22

מה ההבדל העיקרי בין אישור דיגיטלי (Digital certificate) לבין חתימה דיגיטלית (Digital signature)?

- א. אישור דיגיטלי משתמש במפתח פרטי להצפנת הנתונים, וחתימה דיגיטלית מאפשרת זיהוי משתמש.
- ב. אישור דיגיטלי מאמת את זהות המשתמש, וחתימה דיגיטלית מאמתת את שלמות המידע.
- ג. אישור דיגיטלי מצפין נתונים, וחתימה דיגיטלית משמשת לאימות זהות המשתמש.
- ד. אישור דיגיטלי הוא מפתח ציבורי, וחתימה דיגיטלית היא מפתח פרטי.

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 23

לפניכם היגדים המתייחסים לטכנולוגיית VPN.

קבעו לגבי כל אחד מהם אם הוא נכון או לא נכון:

- א) המרכיב המאפשר סודיות (confidentiality) ב־VPN הוא הצפנה (Encryption). נכון / לא נכון
- ב) Data integrity מאפשר לוודא זיהוי משתמש לפני מתן גישה לנתונים. נכון / לא נכון
- ג) האלגוריתמים AES ו־3DES משמשים עבור סודיות (confidentiality), כך שרק הצדדים המורשים יוכלו לפענח את המידע. נכון / לא נכון
- ד) MD5 הוא אלגוריתם המשמש להצפנה של נתונים ב־VPN. נכון / לא נכון

שאלה 24

איזה מנגנון מחבר יחד את ה־policies ואת ה־transform set בהגדרת התצורה (configuration) של IPsec?

- א. ISAKMP policy
- ב. IKE Phase 2
- ג. Crypto Access-Control-Lists
- ד. Crypto map

שאלה 25

מה ההבדל בין Tunnel Mode ל־Transport Mode ב־IPsec?

- א. ב־Tunnel Mode מוצפנים גם כותרות ה־IP וגם חבילת הנתונים (Data-Packet), וב־Transport Mode מוצפן רק תוכן חבילת הנתונים.
- ב. ב־Tunnel Mode מוצפן רק תוכן חבילת הנתונים, וב־Transport Mode מוצפנים גם כותרות ה־IP וגם חבילת הנתונים (Data-Packet).
- ג. ב־Tunnel Mode מוצפנות רק כתובות ה־IP, וב־Transport Mode מוצפן רק תוכן חבילת הנתונים.
- ד. אין הבדל בין Tunnel Mode ל־Transport Mode. שניהם מצפינים רק את תוכן חבילת הנתונים (Data-Packet).

שאלה 26

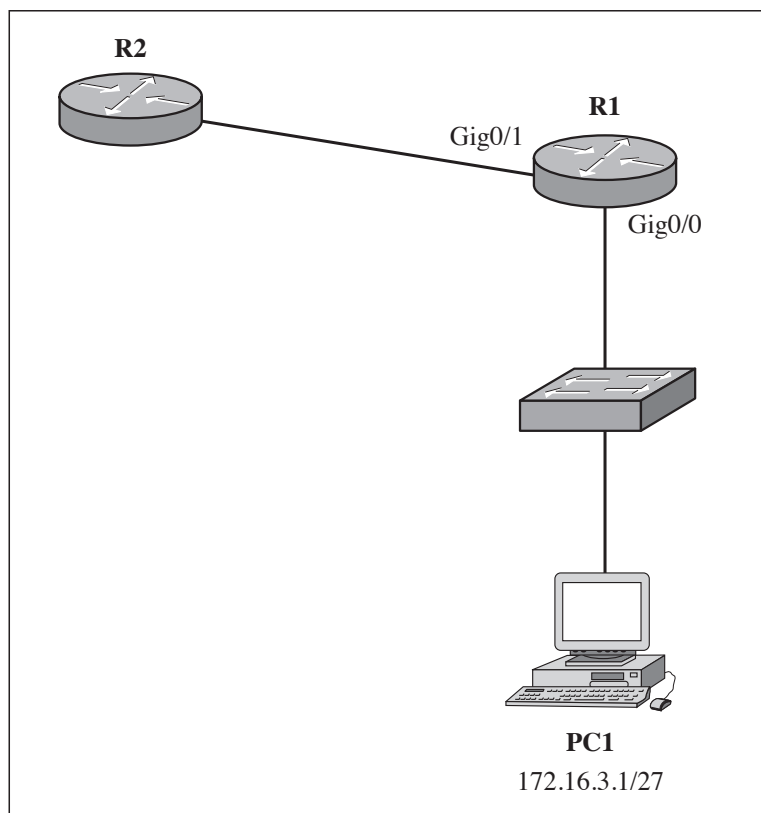
השלימו את הפקודה שתגדיר ממשק במתג Switch-5 כ"אמיין" (trusted), כדי למנוע התקפות DHCP Spoofing ברשת.

Switch-5 (config-if)#ip _____

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 27

לפניכם טופולוגיה מספר 6 ופלט חלקי של הגדרות בנתב R1 (פלט מספר 6).



טופולוגיה מספר 6

```

interface Loopback 1
  Ip address 192.168.1.1 255.255.255.0
!
interface Loopback 2
  Ip address 192.168.2.1 255.255.255.0
!
interface Loopback 3
  Ip address 192.168.3.1 255.255.255.0
!
interface GigabitEthernet0/0
  Ip address 172.16.3.254 255.255.255.224
!
    
```

פלט מספר 6



יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

השלימו את הפקודות שיוגדרו בנתב R1 כדי למנוע גישת SSH ממחשב PC1 לנתב R1, ותתאפשר כל תעבורת נתונים אחרים מכל התקן ברשת לנתב זה.

R1>ena

R1# configure terminal

R1(config)# access-list 110 _____

R1(config)#access-list _____ permit _____

R1(config)#interface _____

R1(config-if)#ip access-group _____

שאלה 28

לפניכם שלוש הגדרות למערכות או מנגנונים שנועדו לאבטחה. השלימו, מתוך מחסן המילים שנמצא מתחת לשאלה, את שלושת השמות של המערכות ומנגנוני האבטחה, בהתאם להגדרתם.

_____ היא מערכת שמנתחת את התעבורה הנכנסת ו/או היוצאת לרשת, ומחליטה אם לאפשר או לחסום את התעבורה שלה.

_____ היא מערכת המנטרת את תעבורת הנתונים ומנתחת אותה, כדי לזהות פעילות חשודה ולהתריע עליה.

_____ היא רשימת כללים המאפשרת את התעבורה ברשת על-ידי הרשאה או חסימה של חבילות נתונים על בסיס קריטריונים שונים.

מחסן מילים: Hash Firewall TLS ACL IDS

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 29

בטבלה שלפניכם מופיעים מאפיינים ותכונות המתייחסים לשירותי האימות TACACS+ ו/או RADIUS. סמנו ✓ בעמודה המתאימה לכל מאפיין או תכונה. אם שני הפרוטוקולים מתאימים, סמנו ✓ בשתי העמודות

RADIUS	TACACS+	מאפיין/תכונה
		הצפנה מלאה של כל תעבורת הנתונים
		אימות דו־כיווני
		שימוש בפרוטוקול UDP בלבד
		תמיכה מלאה ב־Multi-Factor Authentication
		קל להתקנה ודורש פחות משאבי מערכת
		אימות באמצעות AAA (חלקי או מלא)

שאלה 30

כדי להתחבר לתוכנה של מדיה חברתית המאפשרת שיתוף מידע אישי, נדרש מהמשתמש לבצע זיהוי ביומטרי באמצעות טביעת אצבע, להזין סיסמה, ולהקליד קוד שנשלח לדואר האלקטרוני שלו.

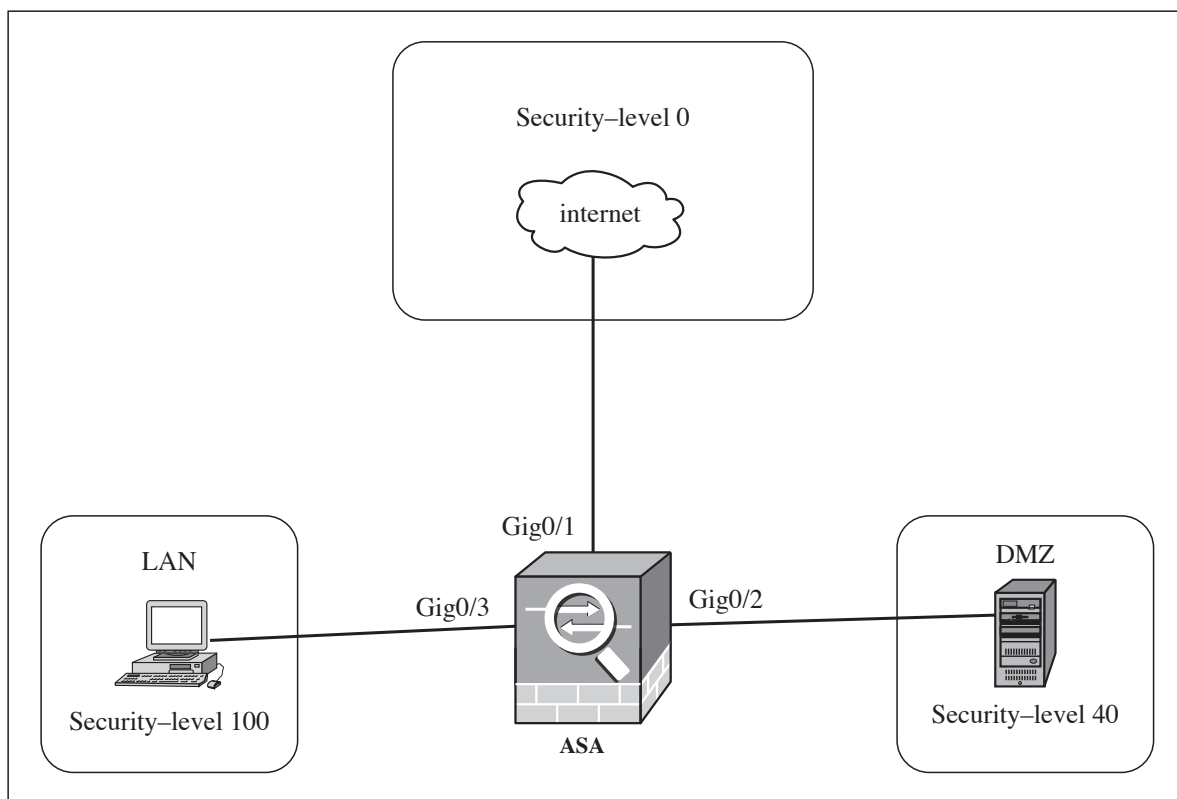
איזה סוג של אימות נדרש המשתמש לבצע?

- א. Risk-Based Authentication (RBA)
- ב. Single Factor Authentication (SFA)
- ג. Two-Factor Authentication (2FA)
- ד. Multi-Factor Authentication (MFA)

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלות 31–33 מתייחסות לטופולוגיה מספר 7.

לפניכם טופולוגיה מספר 7, הכוללת רמות אבטחה תוך שימוש ב־ASA (Adaptive Security Appliance).



טופולוגיה מספר 7

שאלה 31

איזה משפט מתאר את תנועת הנתונים בממשקים המחוברים ל־ASA בטופולוגיה מספר 7?

- תנועה הנשלחת מה־LAN ומה־internet ל־DMZ מתייחסת למצב "תנועה נכנסת" (inbound).
- תנועה הנשלחת מה־DMZ ומה־LAN ל־internet מתייחסת למצב "תנועה יוצאת" (outbound).
- תנועה הנשלחת מה־LAN ל־DMZ מתייחסת למצב "תנועה נכנסת" (inbound).
- תנועה הנשלחת מממשק (יציאה) המחובר לרמת אבטחה גבוהה לכיוון רמת אבטחה נמוכה, מתייחסת תמיד למצב "תנועה נכנסת" (inbound).

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 32

בטופולוגיה מספר 7, כיצד ניתן למנוע גישה מה-DMZ לאינטרנט?

- (א) יש להגדיר ACL שמונע גישה מהממשק.
- (ב) יש לשנות את רמת האבטחה של ה-DMZ ל-100.
- (ג) יש להוסיף ביציאה לאינטרנט נתב שיוגדר בו פרוטוקול מתקדם מסוג Link state.
- (ד) להוסיף מתג משכבה 3 שיחבר בין ה-ASA ל-DMZ.

שאלה 33

לפניכם היגדים המתייחסים לטופולוגיה מספר 7.

קבעו לגבי כל אחד מהם אם הוא נכון או לא נכון:

- (א) אם נשנה את רמת האבטחה (Security level) של ה-DMZ ל-100, תתאפשר תעבורה חופשית מה-DMZ לכל רשת אחרת עם רמת אבטחה נמוכה יותר, בהתאם לברירת המחדל. נכון / לא נכון
- (ב) ניתן לאפשר גישה מהאינטרנט ל-DMZ בלי להגדיר ACL (Access Control List) נוסף ב-ASA. נכון / לא נכון
- (ג) ASA מונע באופן אוטומטי את כל תעבורת ה-DHCP כדי להגן על הרשת מהתקפות DHCP Spoofing. נכון / לא נכון
- (ד) כדי לאפשר גישה מאובטחת מה-LAN ל-internet, ניתן להשתמש בפרוטוקול HTTPS. נכון / לא נכון
- (ה) בדרך כלל, נהוג להגדיר ל-DMZ רמת אבטחה (Security level) בינונית (למשל 40) ולאינטרנט רמת אבטחה נמוכה (למשל 0), כדי להבטיח גישה מבוקרת מהאינטרנט לשרתים ב-DMZ. נכון / לא נכון

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 34

לפניכם **פלט מספר 7**, המכיל הגדרות שנכתבו בנתב Tikshuv:

```
Tikshuv(config)#crypto isakmp policy 50
Tikshuv(config-isakmp)#authentication pre-share
Tikshuv(config-isakmp)#hash sha
Tikshuv(config-isakmp)#encryption 3des
Tikshuv(config-isakmp)#group 5
Tikshuv(config-isakmp)#lifetime 6200
Tikshuv(config-isakmp)#exit
```

פלט מספר 7

(א) מה תפקידה של הפקודה crypto isakmp policy 50 בתצורה של **פלט מספר 7**:

1. להגדיר את מספר העדיפות (Priority) של המדיניות ב-IKEv1.
2. להגדיר את שם המדיניות של IKEv1.
3. להגדיר את סוג ההצפנה להקמת מנהרת VPN מאובטחת.
4. להגדיר את זמן החיים במילי-שניות של מפתח ההצפנה.

(ב) השלימו: **בפלט מספר 7**, המספר _____ מציין את קבוצת הפרמטרים ברמת האבטחה של האלגוריתם Diffie-Hellman, המשמש להחלפת מפתחות.

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלות 35–36 מתייחסות לפלט מספר 8.

פלט מספר 8 שלפניכם הוא פלט חלקי של הפקודה show run שנכתבה בנתב R1. כתובת ה-IP של אחד מהממשקים של הנתב היא 10.0.0.1.
בשרת ה-RADIUS שכתובתו 10.0.0.100 מוגדר משתמש tikshuv1 שסיסמתו Student1.

```
hostname R1
enable password routerpass
!
aaa new-model
!
aaa authentication login default group radius
aaa authentication enable default enable
username TikshuvMGR password 0 router123
access-list 1 permit any
!
radius-server host 10.0.0.100 auth-port 1645 key RouterAAPass
!
!
line vty 0 4
access-class 1 in
password 12345
```

פלט מספר 8

שאלה 35

על-פי המתואר בתחילת השאלה ו**פלט מספר 8**, השלימו על גבי הקווים את שם המשתמש ואת הסיסמאות שיש להקליד כדי להתחבר מהמחשב לנתב R1 באמצעות הפרוטוקול Telnet.

```
C:\> telnet 10.0.0.1
Trying 10.0.0.1 ...Open
User Access Verification

Username: _____
Password: _____
Router>enable
Password: _____
Router#
```

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 36

על-פי המופיע ב**פלט מספר 8**, מה יקרה אם הפקודה "aaa authentication login default group radius" תימחק מנתב R1?

- האימות יבוצע רק מול שרת ה-RADIUS.
- האימות יבוצע רק מקומית בנתב.
- לא תהיה אפשרות להתחבר לנתב.
- כל המשתמשים יוכלו להתחבר ללא אימות.

שאלה 37

לפניכם שני משפטים המתארים את השימוש ב-VPN בהצפנה א-סימטרית, כדי לאבטח את סודיות המידע בין שולח המידע למקבלו.

הקיפו בעיגול את המילים המתאימות בכל אחד מהמשפטים.

ההתקן השולח / המקבל **מצפין** את המידע בעזרת מפתח ציבורי / פרטי של השולח / המקבל.
ההתקן השולח / המקבל **מפענח** את המידע בעזרת מפתח ציבורי / פרטי של השולח / המקבל.

שאלה 38

איזו מבין האפשרויות הבאות היא שיטה יעילה למניעת התקפת CAM Table Overflow במתג?

- הגדרת Port Security על כל אחד מהממשקים (interface) במתג (Switch).
- שימוש ב-VLANs כדי לחלק את ממשקי המתג למספר רשתות.
- שימוש בפרוטוקול STP במתג כדי למנוע לולאות בשכבת קישור הנתונים (Data Link Layer).
- הגדלת ה-CAM table בזיכרון של המתג (Switch).

שאלה 39

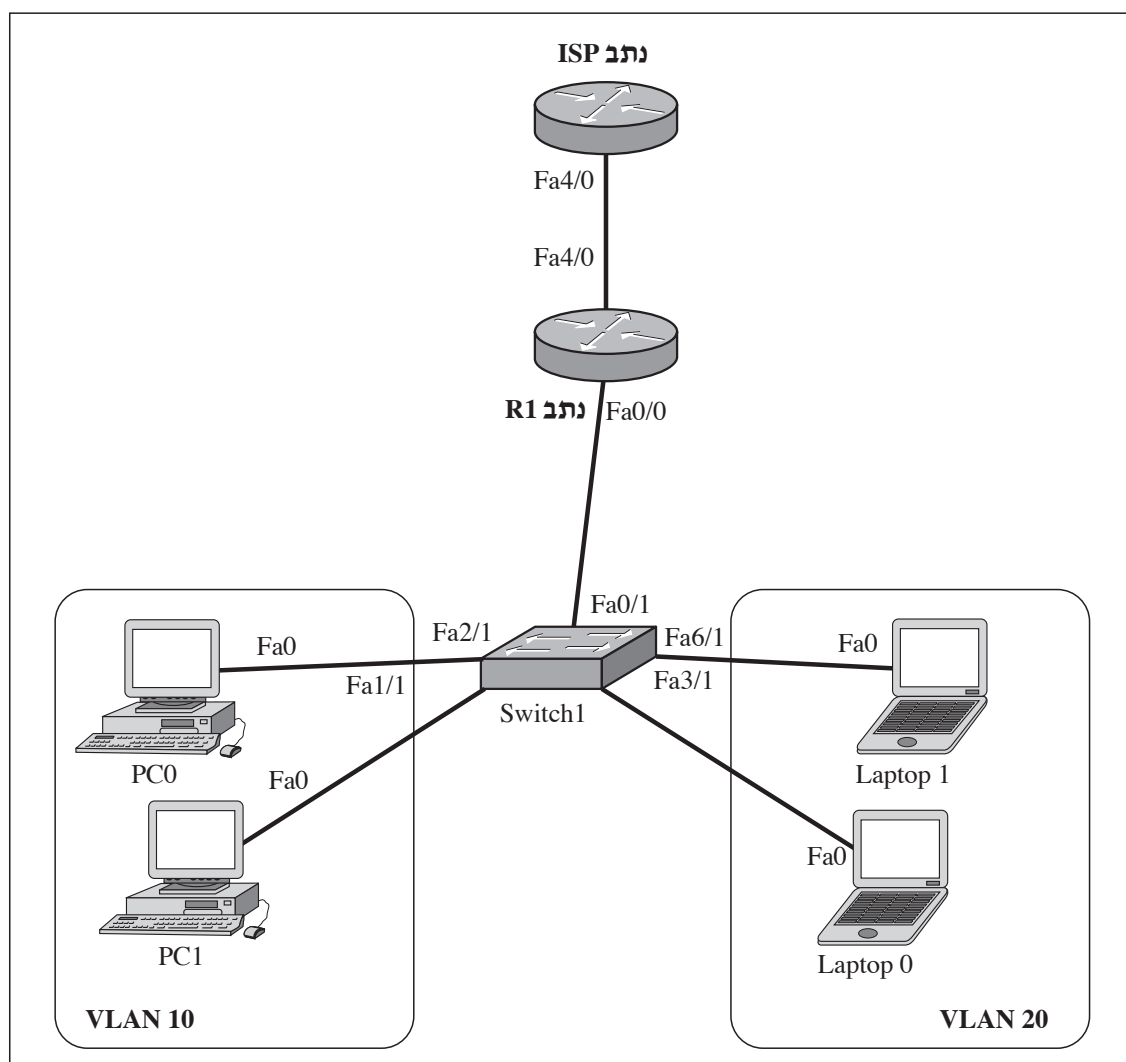
מה פירוש המונח "False Positive" בהקשר של IPS (Intrusion Prevention System)?

- זיהוי נכון של סוג ההתקפה.
- אי זיהוי של התקפה (IPS לא מצליח לזהות את סוג ההתקפה).
- זיהוי שגוי של תעבורה לגיטימית כהתקפה.
- ביצוע פעולה שגויה ברשת בתגובה להתקפה.

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלות 40-41 מתייחסות לטופולוגיה מספר 8 ולפלט מספר 9.

לפניכם טופולוגיה מספר 8 ופלט של נתב R1 (פלט מספר 9). בנתב R1 מוגדר NAT.



טופולוגיה מספר 8

```
R1#show ip interface brief
Interface IP-Address
FastEthernet0/0 unassigned
FastEthernet0/0.10 10.0.0.1
FastEthernet0/0.20 20.0.0.1
FastEthernet1/0 unassigned
Serial2/0 unassigned
Serial3/0 unassigned
FastEthernet4/0 200.1.1.1
FastEthernet5/0 unassigned
R1#
```

פלט מספר 9



יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 40

כאשר המחשבים ב-VLAN 10 מקבלים כתובות בין 200.1.1.2 ל-200.1.1.10, והמחשבים ב-VLAN 20 מקבלים כתובות בין 200.1.1.20 ל-200.1.1.30, ביציאה לכיוון נתב ה-ISP (יש להשתמש ב-overload) –

א) איזה מהממשקים בנתב R1 מוגדרים כ-?inside

ב) מה כתובת ה-IP של הממשק המוגדר כ-?outside בנתב R1

שאלה 41

השלימו, על-פי טופולוגיה מספר 8, את הפקודות החסרות להגדרת הפרוטוקול NAT:

R1# config terminal

R1(config)#access-list 1 permit 10.0.0.0 0.255.255.255

R1 (config)#access-list 2 permit 20.0.0.0 0.255.255.255

R1 (config)#ip nat pool v10 200.1.1.2 200.1.1.10 netmask 255.255.255.0

R1 (config)#ip nat pool v20 200.1.1.20 200.1.1.30 netmask 255.255.255.0

R1 (config)#ip nat inside _____

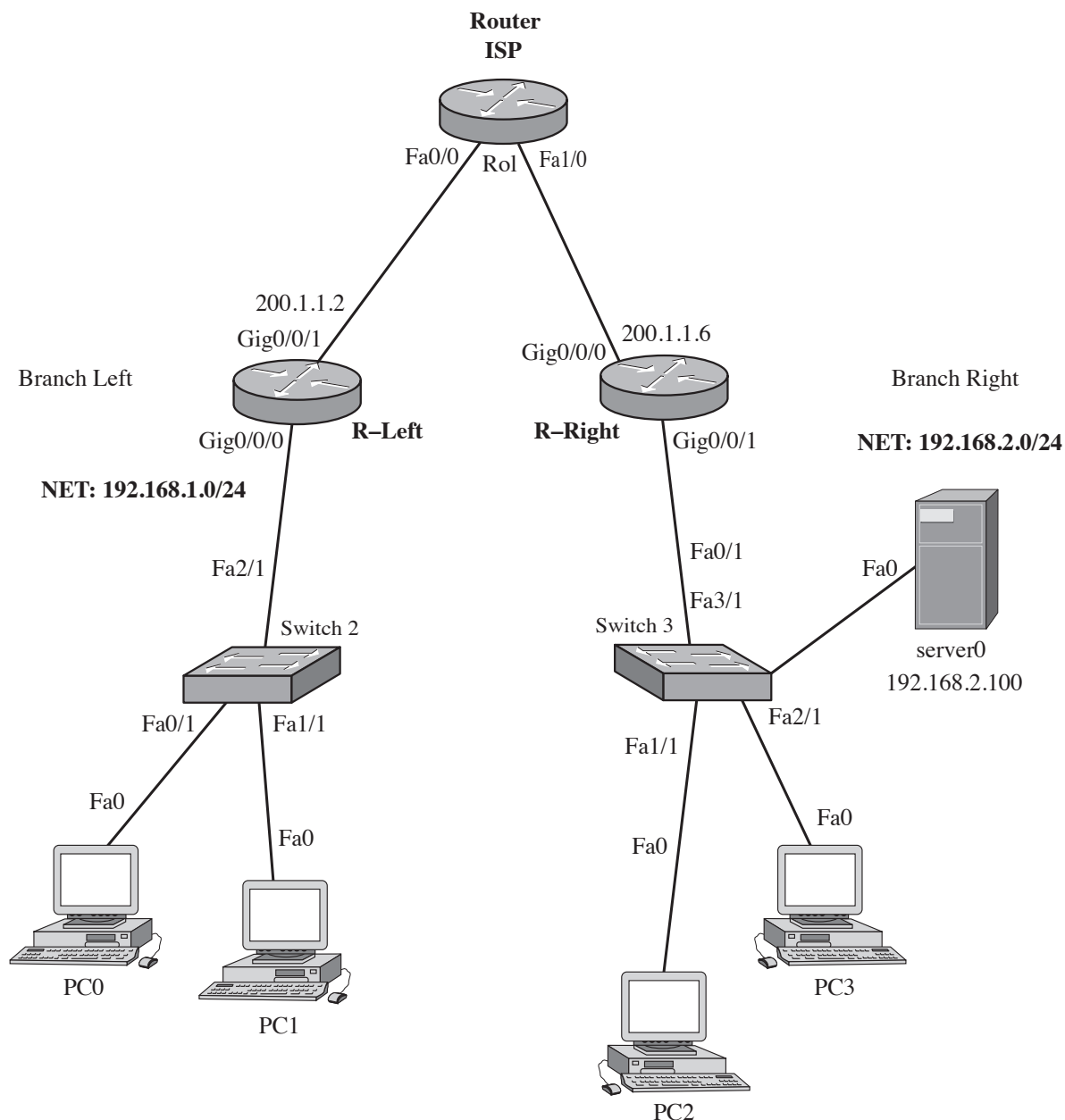
R1 (config)#ip nat inside _____

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

שאלה 42

לפניכם **טופולוגיה מספר 9**, המיועדת להגדרת site to site VPN בין שני אגפים בחברה – בין ממשק (Branch Right) 200.1.1.6/30 לבין ממשק (Branch Left) 200.1.1.2/30.

בעמוד הבא, נתון **פלט מספר 10** עם פקודות הנתב R-Left, ואחריו פקודות חסרות של הנתב R-Right.



טופולוגיה מספר 9

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

```
R-Left(config)#crypto isakmp policy 10
R-Left (config-isakmp)#encr aes 256
R-Left (config-isakmp)#authentication pre-share
R-Left (config-isakmp)#group 5
R-Left (config-isakmp)#exit
R-Left (config)#crypto isakmp key LEFT12345 address 200.1.1.6
R-Left (config)#crypto ipsec transform-set BLeft_BRright esp-aes 256 esp-sha-hmac
R-Left (config)#crypto map VPN-MAP 10 ipsec-isakmp
R-Left (config-crypto-map)#set peer 200.1.1.6
R-Left (config-crypto-map)#set pfs group5
R-Left (config-crypto-map)#set security-association lifetime seconds 86400
R-Left r(config-crypto-map)#set transform-set BLeft_BRright
R-Left (config-crypto-map)#match address 100
R-Left (config-crypto-map)#exit
R-Left (config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R-Left (config)#access-list 100 deny ip any any
R-Left (config)#access-list 150 deny ip 192.168.1.0 0.0.0.255 host 192.168.2.100
R-Left (config)#interface GigabitEthernet0/0/0
R-Left (config-if)#ip address 192.168.1.1 255.255.255.0
R-Left (config-if)#exit
R-Left (config)#interface GigabitEthernet0/0/1
R-Left(config-if)#ip address 200.1.1.2 255.255.255.252
Router(config-if)#crypto map VPN-MAP
```

פלט מספר 10

השלימו את הפקודות החסרות בנתב R-Right (סך הכול – חמש השלמות):

```
R-Right(config)#crypto isakmp policy 10
R-Right (config-isakmp)#encr aes 256
R-Right (config-isakmp)#authentication pre-share
R-Right (config-isakmp)#group 5
R-Right (config-isakmp)#exit
R-Right (config)#crypto isakmp key _____ address _____
R-Right(config)#crypto ipsec transform-set BRight_BLeft esp-aes 256 esp-sha-hmac
R-Right(config)#crypto map VPN-MAP 10 ipsec-isakmp
R-Right (config-crypto-map)#set peer _____
R-Right (config-crypto-map)#set pfs group5
R-Right (config-crypto-map)#set security-association lifetime seconds 86400
R-Right (config-crypto-map)#set transform-set _____
R-Right (config-crypto-map)#match address 100
R-Right (config-crypto-map)#exit
R-Right (config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R-Right (config)#interface GigabitEthernet0/0/0
R-Right (config-if)#ip address _____ 255.255.255.252
R-Right (config-if)#crypto map VPN-MAP
R-Right (config-if)#exit
R-Right (config)#interface GigabitEthernet0/0/1
R-Right (config-if)#ip address 192.168.2.1 255.255.255.0
```

בהצלחה!

זכות היוצרים שמורה למדינת ישראל.

אין להעתיק או לפרסם אלא ברשות משרד החינוך.

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

טיוטה

لا تكتب في هذه المنطقة

لا تكتب في هذه المنطقة

لا تكتب في هذه المنطقة

لا تكتب في هذه المنطقة

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

טיוטה

לא תכתוב באזור זה

לא תכתוב באזור זה

לא תכתוב באזור זה

לא תכתוב באזור זה

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

טיוטה

لا تكتب في هذه المنطقة

لا تكتب في هذه المنطقة

لا تكتب באזור זה

لا تكتب في هذه المنطقة

יישומי ניתוב IP ואבטחה ברשתות קמפוס, אביב תשפ"ה, סמל 735913

טיוטה

لا تكتب في هذه المنطقة

لا تكتب في هذه المنطقة

لا تكتب באזור זה

لا تكتب في هذه المنطقة

מדבקת משגיח

ملصقة مراقب

"איתך בכל מקום, גם בבגרות.
בהצלחה, מועצת התלמידים והנוער הארצית"
"معك في كل مكان، وفي البجروت أيضًا.
بالنجاح، مجلس الطّلاب والشّبيبة القطريّ"

נספח: מילון מונחים
לשאלון 735913, אביב תשפ"ה

תרגום המונח			המונח
אנגלית	רוסית	ערבית	
פרק ראשון – יישומי ניתוב IP			
authentication	Идентификация	التَحَقُّق	אימות
backup	Резервная копия	الحفظ الاحتياطي	גיבוי
topology table	Таблица топологии	جدول طوبولوجيا	טבלת טופולוגיה
routing table	Таблица маршрутизации	جدول توجيه	טבלת ניתוב
neighbors table	Таблица соседних элементов	جدول جيران	טבלת שכנים
routing loops	Петли маршрутизации	حلقات التوجيه	לולאות ניתוב
host	Хост-компьютер	مُضيف	מארח
packet	Пакет	وَجَبَة (دُفْعَة)	מנה
path	Путь	مسار	נתיב
server	Сервер	الخادم	שרת
פרק שני – אבטחה ברשתות קמפוס			
algorithm	Алгоритм	خوارزمية	אלגוריתם
encryption	Шифрование	تشفير	הצפנה
interface	Интерфейс	واجهة	ממשק
RSA key	RSA-ключ	مفتاح RSA	מפתח RSA
switch	Коммутатор/ Переключатель	مفتاح	מתג
router	Маршрутизатор	راوتر	נתב
port	Порт	مَنْفَذ	ממשק
protocol	Протокол	بروتوكول	פרוטוקול
access list	Список доступа	قائمة الوصول	רשימת גישה
network	Сеть	شبكة	רשת
configuration	Конфигурация	مواصفات	תצורה